UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/763,271	02/20/2001	Gerhard Hoffmann	P00,1996	5299

21171	7590	07/15/2005

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER
POLTORAK, PIOTR

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 07/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/763,271	HOFFMANN ET AL.
	Examiner	Art Unit	
	Peter Poltorak	2134	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 April 2005*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-11 and 21-23* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-11 and 21-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____ .

DETAILED ACTION

1. The Amendment, and remarks therein, received on 4/19/2005 have been entered

   and carefully considered.

2. The Amendment introduces new limitations into the originally sole independent

   claims 1 and 11, and introduces new claims 21-23. Claim 4 is cancelled.

   The newly introduced limitation has required a new search and consideration of the

   pending claims. The new search has resulted in newly discovered prior art. New

   grounds of rejection based on the newly discovered prior art follow below.

3. The text of those sections of Title 35, U.S. Code not included in this action can be

   found in a prior office action.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly
claiming the subject matter which the applicant regards as his invention.

4. Claims 1-3 and 5-11 are rejected under 35 U.S.C. 112, second paragraph, as being

   indefinite for failing to particularly point out and distinctly claim the subject matter

   which applicant regards as the invention.

5. The term: "how often" in claims 1, 11 (in preamble) and 21 is not understood. It is not

   clear whether the meaning is directed to the number of times or frequency of a base

   value being increased.

6. Claim 3 recites: "when obtaining the original private key, the predetermined initial value is supplied to a hash function to obtain the base value". The limitation as written <u>may</u> imply that "obtaining the original private key" may precede or be done in parallel to hashing of an initial value (that is to obtaining the base value) but judging from other claims and the specification the process of obtaining the base value is done first, followed by using the base value in obtaining prime numbers used in generation/regeneration of the private key.

7. Claims 3 and 5-10 are rejected by virtue of their dependence.

    Appropriate correction is required.

8. Claims 1-3, 6-11 remain rejected and claims 21-23 are under 35 U.S.C. 103(a) as being unpatentable over *Knuth (Donald E. Knuth, "The art of computer programming, 3rd edition, Vol.1, 1997, ISBN: 0201896834)* in view of *Matyas et al. (U.S. Patent No. 5201000)* and in further in view of *Schneier (Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457)* and in light of *Flanagan (D. Flanagan, "Java in a nutshell", 3rd Edition, 1999, ISBN: 1565924878) and.*

9. As per claim 21 *Knuth* teaches steps of checking whether a value is a prime number and, when the base value is not a prime number, increasing the value by a predetermined increment to obtain a new value, and repeating the step of checking, until a first and a second prime numbers are obtained *(Knuth, "Algorithm P" pg. 147)*.

10. *Knuth* does not teach receiving a predetermined initial value entered by a user, processing the predetermined initial value to obtain a base value for obtaining first and second prime numbers, calculating the public key and the private key using the first prime number and the second prime number.

11. *Matyas et al.* teach receiving a predetermined initial value entered by a user, processing the predetermined initial value to obtain a base value for obtaining first and a second prime numbers, calculating the public and private keys using the first prime number and the second prime number, and erasing the private key *(Matyas et al., Fig. 7, col. 4 lines 58-66, col. 5 lines 22-23, col. 14 lines 20-30, col. 18 lines 49-66, details can be found in the previous Office Action).*

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement receiving a predetermined initial value entered by a user, processing the predetermined initial value to obtain a base value for obtaining first and second prime numbers, calculating the public key and the private key using the first prime number and the second prime number as taught by *Matyas et al's* invention in *Knuth's* invention. One of ordinary skill in the art would have been motivated to perform such a modification in order to generate a public/private key pair using a seed known to a user.

12. *Knuth* and *Matyas et al.* do not explicitly teach calculating the public key using the private key, the first prime number and the second prime number.

13. *Schneier* teaches calculating the public key using the private key, the first prime number, and the second prime number *(Schneier, pg. 467).*

It would have been obvious to one of ordinary skill in the art at the time of applicant's

invention to calculate the public key using the private key, the first prime number and

the second prime number. One of ordinary skill in the art would have been motivated

to perform such a modification in order to utilize a well-known and proven

public/private key generation methods.

14. *Knuth* in view of *Matyas et al.* and *Schneier* do not teach storing an index indicating

how often, in the step of checking, the base value has been increased until the first

prime number or the second prime number is obtained.

15. However, storing an index indicating how often, in the step of checking the base

value has been increased is old and well known in the art as illustrated by *Flanagan*

on pg. 52 for example *("The break Statement", "for" loop in particular)*. Using an

index to store a number representing how many times a test to check whether a

certain condition is met is a fundamental technique in programming and would have

been obvious to one of ordinary skill in the art at the time of applicant's invention.

Any tests of checking whether a number is prime involves multiple computation

(whether the test taught by Knuth, Matyas et al. or more efficient Miller-Rabin test,

Menezes et al., pg. 138-140). As a result one of ordinary skill in the art at the time of

applicant's invention would have been motivated to store an index that allows to

determine how many times an increase of a number (applying certain calculation) is

required in order to derive a first and second primary numbers in order to decrease

complexity of implemented program and increase computing efficiency, especially

since the process of deriving the primary numbers starting at the same base value in

Knuth in view of Matyas et al. is performed repeatedly *(Matyas et al., col. 4 lines 10-*

15).

16. Claims 1, 11 and 23 are substantially equivalent to claim 21; therefore claims 1, 11

and 23 are similarly rejected.

17. As per claims 2 and 3 *Matyas et al.* teach *Key Generation Using a Passphrase*,

wherein a user enters a passphrase. In response, the Key Generate function (47)

parses the input to calculate a hash value (CW) from the input passphrase *(Fig. 13,*

col. 18 lines 49-11). The hash value is passed to the key generation algorithm

(KGA), which generates public and private keys *(Fig. 14 lines 28-36)*.

Using the same hash function when obtaining the original and the regenerated

private keys is implicit.

18. As per claim 6, *Matyas et al.* teach keys being formed according to the RSA method

(col. 12 lines 18-38).

As per claims 7 *Matyas et al.* do not explicitly teach using the MD-5, MD-2 or DES.

However, the choice of MD-5, MD-2 or DES as a hash function would have been

obvious to one of ordinary skill in the art given that they are well known and barring

any unexpected results.

19. As per claims 9-10 *Knuth* in view of *Matyas et al., Flanagan and Schneier* do not

explicitly teach forming a digital signature via electronic data using the regenerated

private key nor does he teach the step authenticating data using said secret

communication key.

Official Notice is taken that it is old and well-known in the art to use a private key to

form a digital signature and a digital signature to provide data authentication. It

would have been obvious to one of ordinary skill in the art at the time of applicant's

invention to form a digital signature via electronic data using the regenerated private

key and to provide data authentication using the digital signature.

One of ordinary skill in the art would have been motivated to perform such a

modification in order to provide non-repudiation.

20. Claim 5 remains rejected under 35 U.S.C. 103(a) as being unpatentable over *Knuth*

(Donald E. Knuth, "The art of computer programming, 3rd edition, Vol.1, 1997, ISBN:

0201896834) in view of *Matyas et al. (U.S. Patent No. 5201000), Flanagan (D.*

Flanagan, "Java in a nutshell", 3rd Edition, 1999, ISBN: 1565924878) and *Schneier*

(Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in

C", 2nd edition, 1996 ISBN: 0471128457) and in further view of *Menezes et al.*

(Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied

cryptography", 1997, ISBN: 0849385237).Matyas et al. (U.S. Patent No. 5201000).

Matyas et al. teach the determination of primacy for any given number as discussed

above.

21. *Knuth* in view of *Matyas et al., Flanagan and Schneier* do not teach the

determination of primacy for any given number carried out according to the method

of Miller-Rabin.

Menezes et al. teach determination of primacy for any given number carried out

according to the method of Miller-Rabin *(Menezes et al., pg. 138-140).*

It would have been obvious to one of ordinary skill in the art at the time of applicant's

invention to use determination of primacy for any given number carried out

according to the method of Miller-Rabin as taught by *Menezes et al.* One of ordinary

skill in the art would have been motivated to perform such a modification in order to

make sure that the numbers identified as prime were always correct *(Menezes et al.*

pg. 140, § 6).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, THIS ACTION IS MADE FINAL. See MPEP §

706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR

1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory.

Any inquiry concerning this communication or earlier communications from the

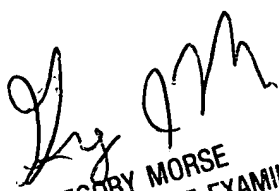examiner should be directed to Peter Poltorak whose telephone number is (571)272-

3840. The examiner can normally be reached Monday through Thursday from 9:00

a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

 If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number

for the organization where this application or proceeding is assigned is 703-872-9306.

 Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at (866) 217-9197 (toll-free).

7/8/05

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100